

*Application*  
*for*  
*United States Patent*

*To all whom it may concern:*

*Be it known that, Sherrie Woodring and Peter Freeland*  
*have invented certain new and useful improvements in*

**ADDRESS MAPPING AND IDENTIFICATION**

*of which the following is a full, clear and exact description:*

**0ADDRESS MAPPING AND IDENTIFICATION**

PRIORITY

[0001] This application claims priority to the provisional U.S. patent application entitled, Address Mapping and Indentification, filed June 13, 2001,  
5 having a serial number 60/297,438, the disclosure of which is hereby incorporated by reference.

FIELD OF THE INVENTION

[0002] The present invention relates generally to mapping fibre channel  
10 frames in order to accomplish monitoring of information being sent and/or received in a device and more particularly, to address mapping in connections when monitoring bidirectional datastreams in a Fibre Channel environment.

BACKGROUND OF THE INVENTION

15 [0003] When displaying service level statistics (e.g. MB/Sec, SCSI IO/Sec) gathered by a probe monitoring a storage area network (SAN), the type of information provided to the end user can often be cryptic at best and as such, difficult to interpret. That is, while a probe is, in fact, connected to a certain port, the data transported on that port is attributed to multiple devices  
20 (e.g., server, tape unit, RAID), each addressed by a unique fibre channel identifier (i.e., FC\_ID). These identifiers are assigned during an initialization sequence between a device and a fibre channel switch, director, or router. The FC\_ID is a 24-bit cryptic address that is difficult for a user to associate with a specific device in the Data Center. In addition, one of the consequences of  
25 letting the topology assign addresses is that any given port may receive a different address from one initialization to the next.

[0004] It would be highly desirable if there were some method whereby a user could view statistics or other data monitored by a probe by the user-defined port name verses the fibre channel address identifier so that at any point in time, a report would be meaningful to an end user seeking to interpret the same. Further, it would be highly desirable to track changes in the fibre channel identifier to the original user-defined port name. Such a methodology has not been proposed in the past as users are required to manually map or assign the fibre channel identifier to the assigned user-defined port name at some subsequent time in order to provide understanding thereto, whereas it would have been much better had the data been generated in a meaningful format in the first place.

[0005] Moreover, users of SANS would be eager to have a method for visually inspecting the type and nature of traffic going through the SAN at any given moment or at any given port location in order to provide the best maintenance and service of the network as possible at any given moment, and throughout the life of the network. In addition, it would be useful for administrators of networks to be able to have a methodology for predicting maximum usage requirements and future needs of each device associated therewith.

[0006] To deliver a highly available and performing storage infrastructure for business critical applications, administrators face many challenges when managing Storage Area Networks (SAN):

- managing data with fewer IT resources,
- managing infrastructure and application changes on a daily basis,
- delivering system and application performance and
- managing flexible deployment of multiple applications across a common infrastructure.

Monitoring the quality of service for a SAN is critical to meeting IT availability and performance goals. It would be desirable to have real-time and trend performance data for critical service-level parameters such as availability, throughput, and utilization. Real-time performance monitoring, with flexible  
5 user-defined thresholds, allows administrators to quickly pinpoint issues that could affect overall SAN performance. Historical trending of performance data extends the administrator's capability to audit and validate service-level agreements. Moreover, as mentioned above, there are the problems in the art relating to how such historical and real-time data and statistics could be presented  
10 by a probe when such a probe is monitoring traffic attributed to multiple devices addressed by 24-bit cryptic fibre channel identifiers.

#### SUMMARY OF THE INVENTION

[0007] In accordance with these and other objects, the present invention  
15 is directed to methods for detecting assignment changes as well as address changes in address identifiers (particularly fibre channel – FC-2- address identifiers such as D\_ID, S\_ID). When such changes are detected, and a probe is in place monitoring at least a portion of a system (i.e., at least one port associated therewith), the detection of a change in address or port assignment  
20 triggers a command to map the change to ensure the user defined port name is always correct. The invention is yet further directed to probes and monitoring systems that are capable of generating data that employ statistics or data referring to user-defined port names at least for purposes of archiving and/or viewing such data or statistics.

25 [0008] There has thus been outlined, rather broadly, the more important features of the invention in order that the detailed description thereof that follows

may be better understood, and in order that the present contribution to the art may be better appreciated. There are, of course, additional features of the invention that will be described below and which will form the subject matter of the claims appended hereto.

5           [0009] In this respect, before explaining at least one embodiment of the invention in detail, it is to be understood that the invention is not limited in its application to the details of construction and to the arrangements of the components set forth in the following description or illustrated in the drawings. The invention is capable of other embodiments and of being practiced and carried  
10 out in various ways. Also, it is to be understood that the phraseology and terminology employed herein, as well as the abstract, are for the purpose of description and should not be regarded as limiting.

          [0010] As such, those skilled in the art will appreciate that the conception upon which this disclosure is based may readily be utilized as a basis for the  
15 designing of other structures, methods and systems for carrying out the several purposes of the present invention. It is important, therefore, that the claims be regarded as including such equivalent constructions insofar as they do not depart from the spirit and scope of the present invention.

## 20                   BRIEF DESCRIPTION OF THE DRAWINGS

          [0011] Figure 1 is a diagram of a typical storage area network and associated devices.

          [0012] Figure 2 is a diagram of a probe system according to the present invention.

25           [0013] Figure 3 is an architecture employed in one embodiment of a probe system according to the present invention.

[0014] Figure 4 is an architecture employed in another embodiment of a probe system according to the present invention.

[0015] Figure 5 is an implementation of a probe system according to the present invention.

5

DETAILED DESCRIPTION OF PREFERRED  
EMBODIMENTS OF THE INVENTION

[0016] According to a preferred embodiment of the present invention, there is provided a system which monitors a port (often a fibre channel port) with a probe, and a method for the purpose of mapping address identifiers to user-defined port names for storing and viewing service level statistics. A “probe” as used herein can be a software or hardware based collection device that monitors frames on a port. When displaying service level statistics, (e.g. in MB/sec) gathered from a probe, users generally prefer viewing statistics that refer to a user-defined port name as opposed to the address identifier (machine level language) used for the frame. For example, in fibre channel (FC-2) the address identifier is an obscure 3-octet identifier (e.g. 3D 09 EF) that is unique within the address domain of the fabric. When a fabric login (ie. FLOGI) procedure occurs between a fabric switch port and an attached device, such as a server or storage device, the device's FC\_ID is assigned by the switch. The fabric switch or director's Fibre Channel Management Framework Integration “MIB” contains the address identifier (FcAddressId) and the user-defined port name (connUnitPortName). This assignment may change between FLOGI sequences. To detect this change and map the new address identifier to the port name in the stored and viewed statistics, the probe system of the present invention monitors traps from the switch or Director, which may indicate topology changes. When a relevant trap is received, the new address identifier is mapped to the port name for storing and viewing purposes. In some

embodiments, the new address identifier that is associated with a user-defined port name is generated as at least one field for whatever purposes are desired such as for generating reports or for archiving the data. Further details regarding the mapping are given *infra*.

5           [0017] According to a preferred embodiment, the present apparatus and methods include mirroring of both the transmit and receive side of a port in a fibre channel switch or director. Mirroring, in a preferred embodiment, involves either 1) splitting preferably about 10% (or from 2-20% in other  
10           embodiments) of the optical energy signal or light being directed to a particular port, and sending that partial optical signal to a probe that replicates the nature of the data presently associated with that particular port for use as a monitor to the outside world; 2) external fibre channel patch panel that replicates the data for a given fibre channel port to the probe; or 3) internal replication of data within the switch or director to the probe, referred to as *port*  
15           *mirroring*. By replicating the signal, it is possible to keep up-to-the-minute statistics on the nature of data then associated with that particular port by viewing the information provided by the probe. The information could be displayed or stored according to any known mechanism including by graphical representations, time based reports, polling of ports, event-based triggers, and  
20           the like. The present invention provides many benefits over such prior maintenance systems such as "Veritas" which only provide information in terms of the MB/sec only at the port level.

          [0018] By employing the present apparatus and/or methods, it is possible to always have current information in terms of the nature of the data  
25           then associated with a port (i.e. small I/O, voice data, video, etc.) as well as its relative contribution to the total traffic in the switch, director, or router. It is further possible to have a record of the particular traffic at a particular

timeframe so as to permit intelligent decision making by operators as to what devices are contributing to problems experienced by the system.

[0019] Fibre channel systems are most often the directors employed in the present marketplace, and as such, the present invention was contemplated with this in mind. However, the invention could, of course, be adapted to other directors and architectures depending on the desired end use without undue experimentation. Fibre Channel topology can be selected depending on system performance requirements or packaging options. Possible fibre channel topologies include point-to-point, crosspoint switched or arbitrated loop. In any of these fibre channel topologies, SCSI storage devices, such as hard disk storage devices and tape devices, can be used to store data that can be retrieved by a software application. Conventionally, fibre channel storage devices have been directly attached to a fibre channel I/O bus on a server.

[0020] As shown, for example, in Figure 1, there is shown an exemplary configuration for a storage area network including a WAN. According to the present invention, it is possible to determine which device(s) are contributing to traffic (e.g., MB/sec, SCSI IO/sec). It is further possible to determine what type of traffic in terms of read/write/other, transaction vs. large file I/O. Other aspects of the present invention are capable of ascertaining whether any retransmissions are occurring in the network and which device(s) are responsible for such retransmission and to what extent a particular device is impacting the network or device due to such retransmission on a real-time basis if desired for a particular reason. It is further possible to determine availability, throughput and latency for each device. These and other aspects of the present invention are provided by virtue of the inclusion of a probe system that gathers statistics directly from Fibre Channel links. Statistics are gathered per Fibre Channel link and per-FC\_ID (24 bit Fibre Channel ID). The Fibre Channel FC\_ID of a device attached to the Fibre Channel fabric is



an obscure 24-bit, 3-octet identifier. Thus, a probe system according to the present invention preferably associates the FC\_ID with the text name of the fabric port to which the corresponding device is attached. Further details regarding one embodiment of how mapping of addresses according to the present invention can be accomplished are set forth below.

[0021] To obtain the mapping of FC\_ID-to-fabric port, a probe can use, for example, Internet Protocol (IP) to communicate with a Simple Network Management Protocol (SNMP) agent in an fabric switch. To track changes to this mapping, a probe sets itself up to receive SNMP traps which indicate that a change in mapping may have occurred.

[0022] Version 2.2 of the Fibre Alliance (fcmgmt) Management Information Block (MIB) (the content of which is incorporated herein by reference in its entirety) should preferably be supported by the fabric switches of the present invention since version 2.2 is most widely supported by commercial devices. However, the same information is available in other versions of the MIB as well, and version 2.2 is being used merely for the sake of simplicity and the invention is not limited thereto.

[0023] A connUnit MIB table describes each switch in the fabric. For each *switch* in the fabric, the following MIB values are read:

- Switch WWN - connUnitGlobalId
- Switch Name - connUnitName
- Switch Model Name - connUnitProduct
- Switch Info – connUnitInfo

[0024] A connUnitPort MIB table describes each port in the fabric. For each *fabric port* in the fabric, the following MIB values are read:

- Physical Port Number - connUnitPortPhysicalNumber

- Port Name - connUnitPortName
- Port Type - connUnitPortType
- Port Speed - connUnitPortSpeed
- Port Transmitter Type - connUnitPortTransmitterType

5

[0025] The physical port number is preferably included, because this parameter is used to associate the FC\_ID of the attached device to the port name.

10 [0026] The port name is desirable, because all displayed references to the fabric port and any device connected to it will generally make use of it. If the port name is uninitialized, an alternative port name can be created from the switch name, port physical number, and the remaining descriptive switch and port parameters.

15 [0027] A connUnitLink MIB table describes connections between the fabric switch and remote devices. For each *remote device* connected to the switch, the following MIB values are read:

- Fabric Port Physical Port Number - - connUnitLinkPortNumberX
- Port FC\_ID - connUnitLinkConnIdY

20 [0028] The fabric port physical number is matched to a physical port number read from the connUnitPort table, to associate the FC\_ID of the connected device with the information about the fabric port read from the port table.

25 [0029] In order to track dynamic changes to the fabric, the probe system of the present invention creates an entry in the trapReqTable (trap request table). The following values can be set, for example, for the entry:

- trapReqIpAddress - IP address of the management system

- trapReqPort - SNMP trap port for the management system
- trapReqFilter - alert(3)
- trapReqRowState - rowActive(3)

5 The following traps are acted upon:

- connUnitStatusChange
- connUnitPortStatusChange

10 [0030] Some fabric switches may also implement connUnitEventTraps reflecting configuration and/or topology events in the fabric. In such cases, these traps would be received as well.

15 [0031] If a connUnitStatusChange trap indicates a connUnitStatus of ok or a connUnitState of online, information in corresponding entries in connUnitTable, connUnitPortTable, and connUnitLinkTable are read from the switch agent's MIB again, and the probe system's state is preferably updated to reflect any changes.

20 [0032] If a connUnitPortStatusChange trap indicates a connUnitPortStatus of ok or a connUnitPortState of online, information in corresponding entries in connUnitPortTable and connUnitLinkTable are read from the switch agent's MIB again, and the probe system's state is updated to reflect any changes.

[0033] As access to storage grows exponentially, a probe system according to the present invention enables the administrator to manage availability and performance by:

25

- Driving towards 100% uptime through proactive monitoring - knowing something will fail before it does,

- Isolating problems instantaneously through real-time problem detection and reporting,
- Monitoring I/O performance based on changing traffic types,
- Planning infrastructure changes and growth through historical performance visibility, and
- Knowing the impact of application and infrastructure changes proactively.

[0034] A probe system according to the present invention collects service-level performance data by directly monitoring the Fibre Channel port I/O. Fibre Channel ports that could significantly impact availability and performance of the SAN include:

- E\_Ports used for Inter-switch links (ISL) between edge switches and core directors or between core directors,
- N\_Ports on a RAID subsystem that are shared between one or more servers and applications,
- E\_Ports extended over the WAN using GigE or ATM transport for remote data access, disk mirroring, and data replication.

[0035] A probe system according to the present invention enables intelligent monitoring through user-definable threshold levels that ensure that those who need to know about critical events are notified in real time and when attention is required. A probe system according to the present invention provides service-level parameters at both the FC port and device (e.g., server, LUN) level. Performance visibility at the server level across a shared SAN port is an important aspect to the present invention as well as detailed port level monitoring. By having such information, an end user is able to properly plan, implement and managing SAN connectivity and performance. A probe system according to the present invention answers critical service-level question such as:

- Who's contributing to the traffic (in MB/sec, SCSI IO/sec)?

- What type of traffic (read/write percentages, transaction vs large file operations)?
- When does the service degrade due to latency? Who contributes to this degradation?
- 5 • Who's experiencing throughput problems (i.e., retransmissions)?
- Who's experiencing availability (i.e., connectivity) problems (e.g., link resets)?

[0036] As shown in Figure 2, it is possible to employ a *dedicated*  
10 *probe* that accesses the Fibre Channel port via an optical splitter (e.g., 90/10 splitter) and cannot be switched through software control. Alternatively, there can be provided a *roaming probe* that can be switched from port to port through *port mirroring*, internal or external to the switch or director. The probe system according to the present invention is generally capable of  
15 mirroring any E\_Port, N\_Port, or GigE port for bi-directional monitoring.

[0037] According to the proposed implementation of the present invention described in Figures 3 and 4, the SAN has no single point of failure within a Data Center. However, should the Primary Data Center experience multiple failures (e.g., redundant primary storage fails) or the entire Data  
20 Center goes off-line (e.g., disaster), then the Backup Data Center can assume partial or full operations through mirrored disks and/or redundant servers.

[0038] As shown, for example, in Figure 5, service quality of the SAN in terms of utilization and availability at the port and device (e.g., Server) level for shared ISL ports is provided. Such an arrangement enables the SAN  
25 manager to plan and implement network moves/adds/changes and manage network service levels. Moreover, multiple ports are provisioned for a given RAID subsystem. A single N\_Port to a RAID may transport data to/from multiple volumes accessed by multiple servers. To properly plan and

implement network moves/adds/changes, the SAN manager needs to determine if a RAID port is oversubscribed or under-subscribed. If oversubscribed, he/she needs to know who is contributing to the load (e.g., which servers). Further, as shown in Figure 5, WAN ports are capable of being monitored.

[0039] As used herein, the following terms are intended to have the meanings set forth below which are believed to be consistent with known Fibre Channel technology:

**8B/10B**

The IBM patented encoding method used for encoding 8-bit data bytes to 10-bit Transmission Characters. Data bytes are converted to Transmission Characters to improve the physical signal such that the following benefits are achieved: bit synchronization is more easily achieved, design of receivers and transmitters is simplified, error detection is improved, and control characters (i.e., the Special Character) can be distinguished from data characters.

**Arbitrated Loop**

One of the three Fibre Channel topologies. Up to 126 NL\_Ports and 1 FL\_Port are configured in a unidirectional loop. Ports arbitrate for access to the Loop based on their arbitrate loop physical address (AL\_PA). Ports with lower AL\_PA's have higher priority than those with higher AL\_PA's.

**BB\_Credit**

Buffer-to-buffer credit value. Used for buffer-to-buffer flow control, this determines the number of frame buffers available in the port it is attached to, i.e., the

maximum number of frames it may transmit without receiving an R\_RDY.

**Buffer-to-Buffer** (flow control) - This type of flow control deals only with the link between an N\_Port and an F\_Port or between two N\_Ports. Both ports on the link exchange values of how many frames it is willing to receive at a time from the other port. This value becomes the other port's BB\_Credit value and remains constant as long as the ports are logged in. For example, when ports A and B log into each other, A may report that it is willing to handle 4 frames from B; B might report that it will accept 8 frames from A. Thus, B's BB\_Credit is set to 4, and A's is set to 8.

Each port also keeps track of BB\_Credit\_CNT, which is initialized to 0. For each frame transmitted, BB\_Credit\_CNT is incremented by 1. The value is decremented by 1 for each R\_RDY Primitive Signal received from the other port. Transmission of an R\_RDY indicates the port has processed a frame, freed a receive buffer, and is ready for one more. If BB\_Credit\_CNT reaches BB\_Credit, the port cannot transmit another frame until it receives an R\_RDY.

**B\_Port** A bridge port is a fabric inter-element port used to connect bridge devices with E-ports on a switch. The B\_Port provides a subset of the E\_port functionality.

**Class n** Fibre Channel Classes of service. Fibre channel (FC-2) defines several Classes of service. The major difference

between the Classes of service is the flow control method used. The same pair of communicating ports may use different Classes of service depending on the function/application being served. Note that Class 1 service is not well defined/supported for FC over WAN configurations. All FC over WAN discussions in this document are for the transport of Class 2 or Class 3 traffic (and Class F traffic - see below).

**Class 1**

A method of communicating between N\_Ports in which a dedicated connection is established between them. The ports are guaranteed the full bandwidth of the connection and frames from other N\_Ports may be blocked while the connection exists. In-order delivery of frames is guaranteed. Uses end-to-end flow control only.

**Class 2**

A method of communicating between N\_Ports in which no connection is established. Frames are acknowledged by the receiver. Frames are routed through the Fabric, and each frame may take a different route. In-order delivery of frames is not guaranteed. Uses both buffer-to-buffer flow and end-to-end flow control. Class 2 & 3 are used most often in the industry.

**Class 3**

Class 3 is very similar to Class 2. The only exception is that it only uses buffer-to-buffer flow control. It is referred to a datagram service. Class 3 would be used when order and timeliness is not so important, and when the ULP itself handles lost frames efficiently. Class 3 is



the choice for SCSI. Class 2 & 3 are used most often in the industry.

**Class 4**

Class 4 provides fractional bandwidth allocation of the resources of a path through a Fabric that connects two N\_Ports. Class 4 can be used only with the pure Fabric topology. One N\_Port will set up a Virtual Circuit (VC) by sending a request to the Fabric indicating the remote N\_Port as well as quality of service parameters. The resulting Class 4 circuit will consist of two unidirectional VCs between the two N\_Ports. The VCs need not be the same speed.

Like a Class 1 dedicated connection, Class 4 circuits will guarantee that frames arrive in the order they were transmitted and will provide acknowledgement of delivered frames (Class 4 end-to-end credit). The main difference is that an N\_Port may have more than one Class 4 circuit, possibly with more than one other N\_Port at the same time. In a Class 1 connection, all resources are dedicated to the two N\_Ports. In Class 4, the resources are divided up into potentially many circuits. The Fabric regulates traffic and manages buffer-to-buffer flow control for each VC separately using the FC\_RDY Primitive Signal. Intermixing of Class 2 and 3 frames is mandatory for devices supporting Class 4.

**Class 5**

The idea for Class 5 involved isochronous, just-in-time service. However, it is still undefined, and possibly

scrapped altogether. It is not mentioned in any of the FC-PH documents.

**Class 6**

Class 6 provides support for multicast service through a Fabric. Basically, a device wishing to transmit frames to more than one N\_Port at a time sets up a Class 1 dedicated connection with the multicast server within the Fabric at the well-known address of hex'FFFFF5'. The multicast server sets up individual dedicated connections between the original N\_Port and all the destination N\_Ports. The multicast server is responsible for replicating and forwarding the frame to all other N\_Ports in the multicast group. N\_Ports become members of a multicast group by registering with the Alias Server at the well-know address of hex'FFFFF8'. The Class 6 is very similar to Class 1; Class 6 SOF delimiters are the same as used in Class 1. Also, end-to-end flow control is used between the N\_Ports and the multicast server.

**Class F service** As defined in FC-FG, a service which multiplexes frames at frame boundaries that is used for control and coordination of the internal behavior of the Fabric.

**Class N service** Refers to any class of service other than Class F.

**Command Tag Queuing**

A SCSI-2 feature that is used when the initiator wants to send multiple commands to the same SCSI address or LUN. Tagged queues allow the target to store up to 256 commands per initiator. Without tagged queues, targets

could support only one command per LUN for each initiator on the bus. Per the SCSI-2 specification, tagged queue support by targets is optional.

5       **Cut-through**    (routing) In a LAN switching environment the action of transmitting a frame on one port before all of that frame has been received from another port. Done for reasons of speed rather than integrity. Cf store and forward.

10       **E\_Port**        As defined in FC-SW-2, a Fabric expansion port which attaches to another E\_Port to create an Inter-Switch Link.

15       **Hard Zone**     A Zone which is enforced by the Fabric, often as a hardware function. The Fabric will forward frames amongst Zone Members within a Hard Zone. The Fabric prohibits frames from being forwarded to members not within a Hard Zone. Note that well-known addresses are implicitly included in every Zone.

20       **Hub (FC)**       Hubs allow multiple FC ports (NL\_Ports and at most one FL\_Port) to interconnect in a FC-AL (arbitrated loop) topology. Hubs are often manageable, support the cascading of multiple Hubs to form larger FC-AL loops, and provide hot-plug for the FC-AL ports. Hubs may also provide full non-blocking performance on all ports by intelligently and dynamically allowing ports to  
25        arbitrate/communicate with each other independent of traffic on other loop ports (a hub/loop trick).

	<b>Initiator</b>	An initiator is a SCSI device that requests an I/O process be performed by another SCSI device (a target).
	<b>iSCSI</b>	A specification that covers the transport of SCSI
5	<b>Fabric</b>	As defined in FC-FG (see reference [7]), an entity which interconnects various Nx_Ports attached to it and is capable of routing frames using only the D_ID information in an FC-frame header. In the FC-SW-2 standard, the term Fabric refers to switches that conform to the SW operational layer.
10	<b>Fabric Element</b>	A Fabric Element is the smallest unit of a Fabric which meets the definition of a Fabric. A Fabric may consist of one or more Fabric Elements, interconnected E_Port to E_Port in a cascaded fashion, each with its own Fabric controller. To the attached N_Ports, a Fabric consisting of multiple Fabric Elements is
15		indistinguishable from a Fabric consisting of a single Fabric Element.
	<b>F_Port</b>	a port in the fabric where an N_port or NL_port may attach
20	<b>FC</b>	Fibre Channel (See FC-FS.)
	<b>FC-0</b>	FC protocol layer defining physical characteristics (signaling, media, tx/rx specifications - See FC-PI)
	<b>FC-1</b>	FC protocol layer defining 8B/10B character encoding and link maintenance (see FC-FS)

- 5      **FC-2**      FC protocol layer defining frame formats, sequence/exchange management, flow control, classes of service, login/logout, topologies, and segmentation/re-assembly.
- FC-3**      Services for multiple ports on one node (See FC-FS).
- FC-4**      Upper Layer Protocol (ULP) mapping. FC-4 defines how ULPs are mapped over FC-FS. Popular ULPs include SCSI, FICON, IP, and VI.
- 10      **FC-AL-2**      NCITS Project 1133-D, *Fibre Channel Arbitrated Loop* - 2
- FC-BB**      NCITS Project 1238-D, *Fibre Channel Backbone*. The FC-BB specifications will provide the necessary mappings bridge between physically-separate instances of the same network definition, including MAC address mapping & translation, configuration discovery, management facilities and mappings of FC Service definitions. Currently the FC-BB specification covers only ATM and packet over SONET/SDH networks.
- 15
- 20      **FC-BBW\_ATM**      An ATM WAN interface specification that interfaces with Fibre Channel Switches on one side and ATM on the other.
- FC-BBW\_SONET/SDH**
- 25      A SONET/SDH WAN interface specification that interfaces with Fibre Channel Switches on one side and SONET/SDH on the other.

**FC-FLA** NCITS TR-20, *Fibre Channel Fabric Loop Attachment*

**FC-FS**

NCITS Project 1311D, *Fibre Channel Framing and Signaling Interface*

5

**FC-GS-3** NCITS Project 1356D, *Fibre Channel Generic Services*  
- 3

**FC-PH** NCITS Project 755-M, *Fibre Channel Physical and Signaling Interface*. FC-PH-3 was the last version of the FC-PH series of specs. Physical and signaling interfaces are now covered in FC-PI and FC-FS.

10

**FC-PI** NCITS Project 1306-D, *Fibre Channel - Physical Interface*.

**FC-PLDA** NCITS TR-19, *Fibre Channel Private Loop, SCSI Direct Attach*

15

**FC-TAPE** NCITS Project 1315D, *Fibre Channel - Tape Technical Report*

**FC-VI** NCITS Project 1332D, *Fibre Channel - Virtual Interface Architecture Mapping*. This goal of FC-VI is to provide a mapping between FC and VIA (Virtual Interface Architecture) "to enable scalable clustering solutions."

20

**FCP** X3.269-1996, *Fibre Channel Protocol for SCSI*

**FCP-2** Fibre Channel Protocol for SCSI, second version.

**FC-4** Fibre Channel Layer 4 mapping layer. (See FC-FS.)

**FL\_Port** a port in fabric where an N\_Port or an NL\_Port may attach

**Fabric Login (FLOGI)**

5 Fabric Login Extended Link Service. (See FC-FS.). An FC-2 defined process used by N/NL\_Ports to

**Frame** The basic unit of communication between two N\_Ports. Frames are composed of a starting delimiter (SOF), a header, the payload, the Cyclic Redundancy Check (CRC), and an ending delimiter (EOF). The SOF and EOF contain the Special Character and are used to indicate where the frame begins and ends. The 24-byte header contains information about the frame, including the S\_ID, D\_ID, routing information, the type of data contained in the payload, and sequence/exchange management information. The payload contains the actual data to be transmitted, and may be 0-2112 bytes in length. The CRC is a 4-byte field used for detecting bit errors in the received frame.

10

15

20

**G\_Port** A generic Fabric\_Port that can function either as an E\_Port or an F\_Port.

25 **GL\_Port** A generic Fabric\_Port that can function either as an E\_Port or an FL\_Port.

5	<b>GBIC</b>	Gigabit Interface converter, these devices can be obtained in copper DB9, SSDC and Fibre Optic type connection. GBICS are hot swappable allowing reconfiguration to take place on a live system with no down time
	<b>HBA</b>	(host bus adapter) - this is the card that fits into the server workstation to provide the interface between the processor and Fibre Channel connection (loop, fabric)
10	<b>Hunt Group</b>	A set of N_Ports with a common alias address identifier managed by a single node or common controlling entity. However, FC-FS does not presently specify how a Hunt Group can be realized.
15	<b>Load Balancing</b>	A network feature that attempts to "balance" WAN traffic over more than one link in such a way as to maximize performance. Note that in some implementations load balancing only attempts to equalize throughput across multiple WAN links.
20	<b>LUN</b>	(SCSI) Logical Unit Number. SCSI targets often support multiple LUNs (e.g. a device controller may manage multiple devices - each a separate LUN).
25	<b>LUN Masking</b>	Method for limiting/granting access to specific LUNs from specific ports (for example, LUN Masking may be based on physical ports or World Wide Names). Similar in concept to zoning, but at a SCSI logical unit level.
	<b>LUN Zoning</b>	Same as LUN Masking.



**N\_Port** a port attached to a node for use with point to point or fabric topology. Generally a port attached to a host or device. N\_Ports communicate with other N\_Ports and with F\_Ports.

5      **NL\_Port** a port attached to a node for use in all three FC topologies (loop, fabric, point-to-point). Generally a port attached to a host or device. NL\_Ports communicate with other NL\_Ports and with FL\_Ports.

**NA** Not Applicable

10

**Optical Carrier Level N (OC-N)**

15

The optical signal that results from an optical conversion of an STS-*N* signal. SDH does not make the distinction between a logical signal (e.g. STS-1 in SONET) and a physical signal (e.g. OC-1 in SONET). The equivalent SDH term for both logical and physical signals is synchronous transport module level M (STM-M), where  $M=(N/3)$ . There are equivalent STM-M signals only for values of  $N=3,12,48$ , and 192.

20

**OC-3** SONET 155.52Mbps standard

**OC-12** SONET 622.08Mbps standard

25      **OC-48** SONET 2.488 Gbps standard

**PLOGI** Port (N\_Port) Login Extended Link Service (See FC-FS.)

**Point Multi-Point**

A topology where one unit can communicate with multiple units.

5

**Point-to-Point** A topology where two points communicate

**Port** An access point in a device where a link attaches

10 **Port (N\_Port) Login (PLOGI)**

An FC-2 defined login procedure used by N\_Ports (e.g. hosts and devices) to register (identify) with each other and exchange parameters before communication may occur for ULPs.

15

**Private Loop** An Arbitrated Loop which stands on its own, i.e., it is not connected to a Fabric.

20

**Private NL\_Port** An NL\_Port which only communicates with other ports on the loop, not with the Fabric. Note that a Private NL\_Port may exist on either a Private Loop or a Public Loop.

25

**Public Loop** An Arbitrated Loop which is connected to a Fabric.

**Public NL\_Port** An NL\_Port which may communicate with other ports on the Loop as well as through an FL\_Port to other N\_Ports connected to the Fabric.

	<b>PVC</b>	(Permanent Virtual Circuit) A pre configured logical connection between two ATM systems.
5	<b>SAM-2</b>	ITS Project 1157D, <i>SCSI Architecture Model - 2</i> (See 2.3.)
	<b>Sequence</b>	A group of related frames transmitted unidirectionally from one N_Port to another.
10	<b>SCSI</b>	Small Computer System Interface, any revision.
	<b>SCSI-3</b>	Small Computer System Interface-3, the SCSI architecture specified by SAM-2 and extended by the companion standards referenced in SAM-2.
15	<b>SCSI-FCP</b>	Fibre Channel protocol for SCSI (refer to FCP, FCP-2 above)
20	<b>SFC</b>	(Simple Flow Control) A mechanism wherein 2 bytes in the PAUSE field in the BBW_Header carries a non-zero value indicating the number of 512-bit time units to pause transmission (used in FC-BBW protocols)
25	<b>SR Flow Control</b>	Selective Retransmission sliding window Flow Control Protocol applied between two BBW_ATM devices used for both flow control and error recovery (used in FC-BBW protocols)

5	<b>Soft Zone</b>	A Zone consisting of Zone Members which are made visible to each other through Client Service requests. Typically, Soft Zones contain Zone Members that are visible to devices via Name Server exposure of Zone Members. The Fabric does not enforce a Soft Zone. Note that well known addresses are implicitly included in every Zone.
10	<b>SVC</b>	Switched Virtual Circuit. A virtual link established through an ATM network. Used to establish the link end-points dynamically as the call is established. The link is removed at the end of the call.
15	<b>Switch</b>	enabling devices for large fabrics. Can be connected together to allow scalability to thousands of nodes
20	<b>Target</b>	A SCSI device that executes a command from an initiator to perform a task. Typically a SCSI peripheral device is the target but a host adapter may, in some cases, be a target.
25	<b>T_Port</b>	A port on INRANGE/Qlogic switches that can be used to cascade/extend switches. T_Ports are not interoperable with other vendor's ports. Note that all INRANGE ports can act as any type (T/F/FL) of port.
	<b>ULP</b>	Upper layer protocol (See FC-FS.). Different communication protocols that can be carried by Fibre Channel.

**WAN** Wide Area Network. A network in which computers are connected to each other over a long distance, using telephone lines and satellite communications.

5

**WDM** Wavelength Division Multiplexing. A method for separating several communication channels within one fibre by using different colors of light to separate the channels

10

**Zoning** A logical separation of traffic between host and resources. By breaking up into zones, processing activity is distributed evenly. Zoning is primarily used for security (e.g. to prevent host access to certain devices).

15

**[0040]** The many features and advantages of the invention are apparent from the detailed specification, and thus, it is intended by the appended claims to cover all such features and advantages of the invention which fall within the true spirits and scope of the invention. Further, since numerous modifications and variations will readily occur to those skilled in the art, it is not desired to limit the invention to the exact construction and operation illustrated and described, and accordingly, all suitable modifications and equivalents may be resorted to, falling within the scope of the invention.

20